Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Advanced Methods to Target and Eliminate Unlawful Robocalls	)	CG Docket No. 17-59
	)	
	)	
Call Authentication Trust Anchor	)	WC Docket No. 17-97

COMMENTS OF COMCAST CORPORATION

Matthew T. Murchison
LATHAM & WATKINS LLP
555 Eleventh Street, NW
Suite 1000
Washington, DC 20004

Kathryn A. Zachem
Beth A. Choroser
Regulatory Affairs

Francis M. Buono
Legal Regulatory

COMCAST CORPORATION
300 New Jersey Avenue, NW
Suite 700
Washington, DC 20001

Brian A. Rankin
Andrew D. Fisher
COMCAST CORPORATION
1701 JFK Boulevard
Philadelphia, PA 19103

July 24, 2019

TABLE OF CONTENTS

Page

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Advanced Methods to Target and Eliminate Unlawful Robocalls	)	CG Docket No. 17-59
	)	
	)	
Call Authentication Trust Anchor	)	WC Docket No. 17-97

COMMENTS OF COMCAST CORPORATION

Comcast Corporation ("Comcast") submits these comments in response to the Third Further Notice of Proposed Rulemaking released on June 7, 2019 in the above-captioned proceedings.[1]

INTRODUCTION AND SUMMARY

Comcast commends the Commission for its ongoing efforts to tackle the problem of illegal and fraudulent robocalls. In the past two years, the Commission has taken a variety of important and timely steps to promote the development and implementation of robocall mitigation technologies, and has provided critical flexibility to voice providers seeking to innovate in this arena for the protection of consumers. The Commission's initiatives include an order in November 2017 authorizing voice providers to block certain types of spoofed calls,[2]

---

1 *See Advanced Methods to Target and Eliminate Unlawful Robocalls, Call Authentication Trust Anchor*, CG Docket No. 17-59, WC Docket No. 17-97, Declaratory Ruling and Third Further Notice of Proposed Rulemaking, FCC 19-51 (rel. June 7, 2019) ("Declaratory Ruling" or "Third FNPRM").

2 *See Advanced Methods to Target and Eliminate Unlawful Robocalls*, Report and Order and Further Notice of Proposed Rulemaking, 32 FCC Rcd 9706 ¶¶ 10, 18 (2017) ("*Robocall Blocking Order*").

active efforts to promote the development and adoption of the end-to-end call authentication standard known as SHAKEN/STIR,[3] and aggressive enforcement actions against individuals and entities engaging in fraudulent spoofed robocalling.[4] And in parallel with these important initiatives at the Commission, other federal agencies and law enforcement authorities have begun ramping up efforts to identify and crack down on bad actors that use abusive calling practices to defraud consumers.[5]

The Commission's latest action in this proceeding—a Declaratory Ruling allowing for broader use of certain blocking techniques, coupled with a Third Further Notice of Proposed Rulemaking ("Third FNPRM") regarding call authentication and the impact on emergency communications—represents another laudable step forward. The Declaratory Ruling is "great news for consumers," as Comcast observed in a statement shortly after the draft ruling's release,

---

3 *See, e.g.*, *Call Authentication Trust Anchor*, Notice of Inquiry, 32 FCC Rcd 5988 (2017) ("*Call Authentication NOI*"); FCC, Press Release, "Chairman Pai Calls on Industry To Adopt Anti-Spoofing Protocols To Help Consumers Combat Scam Robocalls," Nov. 5, 2018, *available at* https://docs.fcc.gov/public/attachments/DOC-354933A1.pdf. ("FCC SHAKEN/STIR Press Release"). SHAKEN (Signature-based Handling of Asserted Information Using toKENs) and STIR (Secure Telephone Identity Revisited) together refer to a framework and set of specifications for verifying and authenticating caller identification for IP-based voice calls. *See Call Authentication NOI* ¶ 5.

4 *See, e.g.*, *Adrian Abramovich*, Forfeiture Order, 33 FCC Rcd 4663 (2018) (imposing a forfeiture penalty of $120 million for violations of Truth in Caller ID requirements); *Philip Roesel d/b/a/ Wilmington Insurance Quotes and Best Insurance Contracts*, Forfeiture Order, 33 FCC Rcd 9204 (2018) (imposing a forfeiture penalty of $82 million for violations of Truth in Caller ID requirements).

5 *See* Fed. Trade Comm'n, "FTC, Law Enforcement Partners Announce New Crackdown on Illegal Robocalls," June 25, 2019, *available at* https://www.ftc.gov/news-events/press-releases/2019/06/ftc-law-enforcement-partners-announce-new-crackdown-illegal (announcing "a major crackdown on illegal robocalls, including 94 actions targeting operations around the country that are responsible for more than one billion calls pitching a variety of products and services including credit card interest rate reduction services, money-making opportunities, and medical alert systems").

since the decision to allow certain forms of blocking on a default basis gives voice providers "another tool that will permit [them] to protect [their] customers by stopping illegal robocalls before they reach [their] customers' phones."[6] Comcast is already making progress towards taking advantage of this new regulatory flexibility for the benefit of consumers. In addition to the substantial robocall mitigation efforts already underway at Comcast—including network-level tools that automatically block tens of millions of illegal and fraudulent robocalls bound for Comcast's customers every month, third-party tools like Nomorobo and Hiya available to Comcast's customers at no additional charge, and aggressive implementation of SHAKEN/STIR—Comcast recently reported that it is actively exploring how to make certain blocking tools available on a default, opt-out basis.[7]

Meanwhile, the Third FNPRM puts forward proposals that will help accelerate the adoption of more robust technologies aimed at identifying and blocking fraudulent spoofing, and asks important questions about how best to avoid blocking emergency communications. As discussed below, Comcast strongly supports the Commission's proposed adoption of safe harbors enabling voice providers to block calls automatically using the SHAKEN/STIR protocol. The Commission not only should permit blocking of calls that fail authentication under the

---

6 John Eggerton, *FCC's Pai Proposed Default Robocall Blocking*, Multichannel News, May 15, 2019, *available at* https://www.multichannel.com/news/fccs-pai-proposes-default-robocall-blocking (quoting statement from Eric Schaefer, Senior Vice President at Comcast).

7 *See* Letter of Eric Schaefer, Senior Vice President and General Manager, Broadband, Automation and Communications, Comcast Cable, to Commissioner Geoffrey Starks, FCC, at 1-4 (July 10, 2019), *available at* https://docs.fcc.gov/public/attachments/DOC-358443A6.pdf. For example, Comcast is developing plans in the short term to convert one of its existing opt-in blocking tools for Xfinity Voice customers—Anonymous Call Rejection—into a default, opt-out feature that remains free of charge. Comcast's Anonymous Call Rejection tool automatically rejects calls where the caller has chosen to block the display of the caller's name and number. *Id.* at 2.

standard, but also should consider additional safe harbors that, among other things, would incentivize broader adoption of the standard. Relatedly, while Comcast would not oppose a reasonably defined mandate for industry implementation of SHAKEN/STIR, Comcast also continues to believe that market forces will increasingly drive widespread adoption and may render a mandate unnecessary. Finally, Comcast supports the creation of a centralized Critical Calls List that voice providers could use to avoid blocking emergency communications, and agrees with commenters that have previously urged the Commission to play a lead role in creating and maintaining that list to ensure its comprehensiveness and to secure access.

DISCUSSION

I. COMCAST SUPPORTS THE COMMISSION'S ONGOING EFFORTS TO FOSTER IMPLEMENTATION AND PRODUCTIVE USE OF SHAKEN/STIR

A. The Commission Should Establish Broad Safe Harbors Enabling Voice Providers to Block Calls Using the SHAKEN/STIR Protocol

The Commission's Third FNPRM correctly recognizes that call authentication based on the SHAKEN/STIR protocol, "amongst its many benefits, will provide a strong basis for call blocking."[8] As Comcast and various other parties have explained, SHAKEN/STIR represents the most promising way of addressing illegal spoofed robocalls in a comprehensive and robust manner—enabling calls to be cryptographically signed by the originating provider and verified by the terminating provider.[9] SHAKEN/STIR accomplishes this feat by taking advantage of

---

8 Third FNPRM ¶ 50.

9 *See* Comments of Comcast Corp., CG Docket No. 17-59, at 6-7 (filed Jul. 3, 2017); *see also, e.g.*, Comments of CTIA, WC Docket No. 17-97, at 1 (filed Aug. 14, 2017) (noting that "[t]he SHAKEN/STIR framework developed by these standard-setting bodies has received widespread acclaim" and "is the appropriate framework for call authentication"); Comments of USTelecom, CG Docket No. 17-59, at 4 (filed Jul. 20, 2018) (noting that "there is strong industry commitment to the deployment of the

technical capabilities enabled by Internet Protocol ("IP")—in particular, the ability to "add[] a SIP header" to IP-based voice transmissions "containing specific information enumerated in the standards," and the ability of IP interconnection points to enable providers to pass such information from one network to another.[10] In light of these capabilities, the Robocall Strike Force found that SHAKEN/STIR "holds considerable promise for repressing the presence of robocalling in the communications ecosystem," as it will "provide a basis for verifying calls, classifying calls, and facilitating the ability to trust caller identity end to end."[11] Comcast thus agrees with the observation in the Third FNPRM that using methods enabled by the SHAKEN/STIR protocol to "block[] calls from numbers that are potentially spoofed could significantly reduce the number of robocalls that many consumers receive while ensuring that any spoofed calls they do receive can be more easily traced back."[12]

Specifically, Comcast supports the Commission's proposal for "a safe harbor for voice service providers that choose to block calls (or a subset of calls) that fail Caller ID authentication under the SHAKEN/STIR framework."[13] Comcast has consistently called for the Commission to adopt such a safe harbor. As explained in our comments in response to the very first Notice of Inquiry in this proceeding, such a safe harbor "would encourage providers to implement SHAKEN and STIR, thereby helping to mitigate the possibility of dramatic increases in abusive

---

SHAKEN and STIR standards," which "should improve the reliability of the nation's communications system by better identifying legitimate traffic").

10 Declaratory Ruling ¶ 21.

11 *See* Robocall Strike Force, Robocall Strike Force Report, at 5 (rel. Oct. 26, 2016), *available at* https://transition.fcc.gov/cgb/Robocall-Strike-Force-Final-Report.pdf.

12 Third FNPRM ¶ 50.

13 *Id.* ¶ 51. The Commission also could consider expanding this safe harbor to include unsigned calls that originate with, and are transported by, providers that are otherwise participating in the SHAKEN/STIR framework.

call rates, while also offering providers the greatest assurance that their efforts would not disrupt legitimate calls or expose them to enforcement action."[14]

Moreover, the Third FNPRM is correct that "a call would fail authentication when the attestation header has been maliciously altered or inserted—in other words, where a malicious actor has tried to inappropriately spoof another number and attempted to circumvent the protection provided by SHAKEN/STIR"—and that a safe harbor is accordingly warranted because "the vast majority of calls blocked in such circumstances [will] be illegitimate."[15] Under the SHAKEN/STIR protocol, the identification of these "authentication failures" can occur only when both the originating and terminating providers have implemented the protocol on their networks for the type of call at issue.[16] Also, the SHAKEN/STIR framework currently enables voice providers to distinguish fraudulently spoofed calls from calls where the caller ID information has been changed for legitimate reasons. And in the unlikely event that voice providers exchanging voice calls using SHAKEN/STIR determine that calls are failing authentication for reasons unrelated to fraudulent spoofing, those providers will have every incentive to work together to address any such issues quickly.

---

14 Comcast July 2017 Comments at 9; *see also* Comments of Comcast Corp., CG Docket No. 17-59, at 5 (filed Sep. 24, 2018) (reiterating Comcast's support for a rule "expressly authorizing voice providers to block unauthenticated calls where authentication fails and the originating and terminating providers have implemented SHAKEN/STIR for the type of call at issue").

15 Third FNPRM ¶ 51.

16 Thus, a call would not "fail authentication" for these purposes where, for instance, an originating rural carrier has not yet implemented SHAKEN/STIR because it has not yet transitioned to an IP network or has not installed IP gateways.

The Commission also should give careful consideration to adopting a "safe harbor for blocking unsigned calls from particular categories of voice service providers."[17] The Commission could consider, for instance, allowing the blocking of unsigned calls from major voice providers that have not implemented SHAKEN/STIR and are not exchanging calls on an authenticated basis by a reasonable date.[18] This approach would be consistent with the Commission's broader efforts to promote SHAKEN/STIR implementation specifically and IP-to-IP interconnection more generally. If major voice providers need to install new gateways to enable IP interconnection and the exchange of authentication information under the SHAKEN/STIR protocol, any cost for such traffic conversion from legacy networks must be borne by those providers—and the Commission should consider expressly stating as such in its eventual order to avoid any confusion. A safe harbor along these lines would provide a powerful incentive for all major voice providers to implement the protocol promptly and ensure their networks are configured in a manner that enables IP headers to be transmitted (a necessary feature of full authentication under the protocol), while avoiding the blocking of unsigned calls from smaller voice providers that may need more time to deploy the technology.

Additionally, the Commission should consider expanding voice providers' ability to block calls based on analytics enabled by SHAKEN/STIR implementation. The Declaratory Ruling that accompanied the Third FNPRM helpfully clarifies that voice providers may employ blocking based on analytics enabled by SHAKEN/STIR implementation on a default, opt-out

---

17 Third FNPRM ¶ 54.

18 Under this approach, the Commission could consider clarifying that a major provider may avoid the blocking of its originated calls by other providers terminating such calls only if the originating provider has implemented SHAKEN/STIR across all of its platforms—so that major providers cannot get by with more limited implementation of the protocol.

basis.[19] But because SHAKEN/STIR is a network-level protocol, much of the potential analytics-based blocking enabled by SHAKEN/STIR implementation may be most efficient to carry out at the network level, without individualized determinations that might vary from subscriber to subscriber. As providers continue to experiment with and develop methods for blocking fraudulent spoofed robocalls based on analytics enabled by SHAKEN/STIR implementation, it is critical that the Commission give providers sufficient regulatory flexibility to deploy effective solutions for consumers.

B. The Commission Should Explore All Options in Promoting Widespread Deployment of SHAKEN/STIR

The Commission has made significant and laudable efforts so far in championing the development of the SHAKEN/STIR protocol and pressing voice providers to implement the protocols quickly. The Commission's 2017 Notice of Inquiry drew significant attention to the ongoing industry efforts to develop the standard and plan for implementation,[20] and the 2018 Report prepared at the Commission's request by the North American Numbering Council helped industry take the critical next step of establishing a governance framework for the protocol.[21] Chairman Pai's letters to voice providers asking about their implementation plans, followed by the summit he convened in May on next steps with SHAKEN/STIR deployment, likewise have

---

19 Declaratory Ruling ¶ 35.

20 *See generally Call Authentication NOI.*

21 *See* NANC Call Authentication Trust Anchor Working Group, "Report on Selection of Governance Authority and Timely Deployment of SHAKEN/STIR" (May 3, 2018), *available at* https://transition.fcc.gov/Daily_Releases/Daily_Business/2018/db0503/DOC-350542A1.pdf; *see also* FCC, Press Release, "Chairman Pai Welcomes Call Authentication Recommendations from the North American Numbering Council" (May 14, 2018), *available at* https://transition.fcc.gov/Daily_Releases/Daily_Business/2018/db0514/DOC-350690A1.pdf.

helped clarify where these industry efforts stand.[22] The Commission's initiatives have undoubtedly made a significant impact in spurring the industry towards broad implementation on an expedited timetable.

Comcast, for its part, continues to pursue an aggressive timeline for implementing SHAKEN/STIR on its network. Earlier this year, Comcast implemented the capability to verify calls that contain a STIR/SHAKEN-compliant signature for the company's entire residential subscriber base—enabling Comcast to sign originating calls and verify terminating calls between its subscribers, and paving the way for the company to interoperate with other voice providers that have implemented such capabilities. In March 2019, Comcast and AT&T successfully accomplished an exchange of authenticated calls in a real-world (non-laboratory) setting using phones on the companies' consumer networks—a feat "believed to be an industry first for calls between separate providers."[23] In April 2019, Comcast began exchanging authenticated calls with T-Mobile as well,[24] and in the coming months Comcast expects to exchange authenticated calls with more providers across the industry.

---

22 *See* FCC, Press Release, "Chairman Pai Calls on Industry To Adopt Anti-Spoofing Protocols To Help Consumers Combat Scam Robocalls" (Nov. 5, 2018), *available at* https://docs.fcc.gov/public/attachments/DOC-354933A1.pdf; FCC, Press Release, "Chairman Pai Convenes SHAKEN/STIR Robocall Summit" (May 13, 2019), *available at* https://docs.fcc.gov/public/attachments/DA-19-413A1.pdf.

23 Comcast Corp., Press Release, "AT&T, Comcast Announce Anti-Robocalling Fraud Milestone Believed To Be Nation's First," Mar. 20, 2019, *available at* https://corporate.comcast.com/press/releases/att-comcast-announce-anti-robocalling-fraud-milestone-believed-to-be-nations-first; *see also* Eli Blumenthal, *Fight Against Robocalls Continues as AT&T, Comcast Complete Test of Verified Call*, USA Today, Mar. 20, 2019, *available at* https://www.usatoday.com/story/tech/2019/03/20/at-t-comcast-say-they-making-progress-fight-against-robocalls/3215621002/.

24 *See* Eli Blumenthal, *T-Mobile, Comcast Turn on Call Verification Between Networks in Latest Robocall Fight*, USA Today, Apr. 17, 2019, *available at*

Of course, Comcast recognizes that the Commission still may wish to do more to encourage other voice providers to implement this technology with the same speed, and appreciates the Commission's suggestion to mandate implementation for all voice providers if major providers do not implement by a date certain.[25] Comcast would not be opposed to such a mandate from the Commission, so long as the Commission is careful to frame the mandate in a thoughtful manner and to set realistic targets.[26]

At the same time, strong market-based incentives will continue to play an important role in motivating voice providers to implement the framework.[27] Given the significant benefits to consumers from the reduction in illegal spoofed robocalls stemming from a voice provider's implementation of SHAKEN/STIR, consumers may well choose a voice provider based in part on whether its service can effectively authenticate calls and verify the authenticity of the calling numbers. Additionally, the ability to identify and address illegal spoofed robocalls using SHAKEN/STIR will help reduce network costs for voice providers associated with the

---

https://www.usatoday.com/story/tech/talkingtech/2019/04/17/t-mobile-comcast-turn-call-verification-fight-robocall-epidemic/3490265002/.

25 *See* Third FNPRM ¶ 71.

26 For instance, the Commission should give careful consideration to how it defines "implementation" for purposes of this mandate, and should tailor the deadlines that might apply under any such mandate based on the definition it adopts. If the Commission were to define "implementation" to mean simply that the provider can sign originating calls and verify terminating calls on its network, thus enabling at least calls between its own subscribers to be fully signed and verified, the Commission could reasonably adopt a relatively condensed timetable. If, on the other hand, "implementation" were defined as the ability to exchange authenticated calls with a certain number of other voice providers, the Commission should consider a somewhat longer timetable. As Comcast has learned from its experiences interoperating with other voice providers, the process can entail thorny technical issues requiring the development of specific solutions that may not readily translate to another provider's network.

27 *See* Comments of Comcast Corp., WC Docket No. 17-97, at 5 (Aug. 14, 2017); *see also Call Authentication NOI* ¶ 14.

transmission of these calls. Also, as more and more providers transition to IP interconnection—an important precondition to full implementation of SHAKEN/STIR by a voice provider—there will be a greater propensity for providers to implement the standard. And if the Commission were to adopt a rule that allows for blocking of unsigned calls in certain circumstances—such as the proposal laid out in the preceding section—a voice provider that may be lagging behind would have an overwhelming incentive to avoid large-scale blocking of its originating calls by moving more quickly to implement the framework.[28] These motivating factors, coupled with continued encouragement from the Commission and other policymakers, may well obviate the need for a mandate.

II. COMCAST SUPPORTS THE CREATION OF A CENTRALIZED CRITICAL CALLS LIST

Comcast also agrees with the Commission that it is vitally important for call-blocking programs to avoid interfering with emergency calls and similarly important communications. Currently, there is no comprehensive, centralized list of originating numbers belonging to emergency service providers and similar callers. But if such a tool were developed, it would enable voice service providers to avoid blocking calls from such entities with greater assurance, particularly as the overall percentage of calls being blocked increases in light of recent Commission reforms and ongoing industry efforts. The Third FNPRM is of course correct that the Commission should "exercise caution" in creating such a tool,[29] particularly to prevent

---

[28] For the same reasons, voice providers likely also would have an incentive to ensure that their implementation of SHAKEN/STIR extends to all calls originating on their platforms—including traffic that certain providers are capable of exchanging in IP but, absent such incentives, might choose not to do so.

[29] Third FNPRM ¶ 64.

misuse by bad actors, though if the tool is properly established and if access is appropriately constrained, the benefits of such a tool likely would outweigh the potential downsides.

The Commission thus should move forward with its proposal to establish a Critical Calls List.[30] Comcast agrees with TNS that the Commission "could be instrumental in gathering the numbers of emergency and other important services" for this purpose,[31] and supports an approach under which such a list would be "centrally maintained,"[32] either by the Commission itself or through a third-party provider chosen through a competitive bidding process.

Under this approach, the Commission could, as a first step, collect all numbers assigned to public safety answering points ("PSAPs") for callbacks or transfers, as well as all numbers used for "reverse 911" communications, Government Emergency Telecommunications Service ("GETS") calls, and other federal, state, and local government emergency outbound communications, for automatic inclusion in the Critical Calls List. All or virtually all calls from such numbers likely qualify as emergency communications, so compiling a comprehensive list of such numbers would be essential for creating a Critical Calls List. For other originating numbers that are often but not always used for emergency communications—such as numbers used by local governments, schools, and the like—the Commission could consider providing a mechanism for such entities to add their numbers to the centralized Critical Calls List.[33]

In creating and maintaining a Critical Calls List, it is vital that access to the list be tightly restricted to avoid misuse by bad actors. If, for instance, information about the outbound

---

30 *Id.* ¶ 63.

31 *Id.* ¶ 65 (quoting Comments of TNS, CG Docket No. 17-59, at 20 (filed July 3, 2017)).

32 *Id.*

33 *See id.* ¶ 66.

numbers used by PSAPs were made widely available, fraudulent spoofers may well attempt to use that information and make it appear as though their calls are coming from 911 call centers.[34] Thus, the Commission should require those who wish to access the Critical Calls List to certify as to their use of the list, similar to the certification requirement that the Commission recently established in connection with its reassigned numbers database.[35] Such a certification could state that the requesting entity provides retail voice services in the United States, employs robocall blocking tools, and is accessing the Critical Calls List solely for the purpose of avoiding the blocking of emergency communications. While there is always a risk with every new tool that bad actors might discover ways to exploit it, keeping the Critical Calls List non-public and tightly guarding access to it will go a long way towards minimizing that risk and ensuring that it remains a useful tool.[36]

---

34 To reduce this risk even further, the Commission could consider limiting the use of the Critical Calls List to calls that are otherwise authenticated using the SHAKEN/STIR protocol. *See* Third FNPRM ¶ 67.

35 *See Advanced Methods to Target and Eliminate Unlawful Robocalls*, Second Report and Order, 33 FCC Rcd 12024 ¶ 26 (2018) (requiring that a caller seeking access to the reassigned numbers database must certify in writing that it "will use the database solely to determine whether a number has been permanently disconnected since a date provided by the caller for the purpose of making lawful calls or sending lawful texts").

36 The Commission also should explore other ways of promoting practices aimed at minimizing misuse of numbers on the Critical Calls List by bad actors. One approach could be to encourage the development of standards under which "emergency" calls could be identified as such in SIP signaling and calls marked appropriately could be allowed to bypass call blocking by voice providers.

CONCLUSION

Comcast applauds the Commission's continued focus on the problem of illegal and fraudulent spoofed robocalls. As the Commission and industry stakeholders continue to make significant strides towards addressing this problem on various fronts, Comcast believes that the proposals discussed above will help bolster protections for consumers against abusive calling practices.

Respectfully submitted,

/s/ Kathryn A. Zachem

Kathryn A. Zachem
Beth A. Choroser
Regulatory Affairs

Francis M. Buono
Legal Regulatory

COMCAST CORPORATION
300 New Jersey Avenue, NW
Suite 700
Washington, DC 20001

Brian A. Rankin
Andrew D. Fisher
COMCAST CORPORATION
1701 JFK Boulevard
Philadelphia, PA 19103

Matthew T. Murchison
LATHAM & WATKINS LLP
555 Eleventh Street, NW
Suite 1000
Washington, DC 20004

July 24, 2019